- What IT services other than security are being offered as a service to state departments?

  The Office of Enterprise Technology (OET) offers many centralized solutions to the serve the business needs of government entities. A catalog of services offered can be found at: **http://www.state.mn.us/portal/mn/jsp/content.do?id=-536890274&agency=OETweb**

- What "external mandates" does the state need to comply with?

  The state has many regulatory and contractual requirements that it needs to comply with, including but not limited to FISMA, HIPAA, PCI DSS, CIPA, FERPA, and IRS tax and other federal mandates.

- Are there currently security services that are provided to state departments?

  OET provides centralized business continuity, vulnerability management, and identity and access management solutions. In addition, there are projects underway to provide newly designed security services. The security initiatives are defined in the:
  - Minnesota Enterprise Security Strategic Plan (**http://www.state.mn.us/mn/externalDocs/OET/Enterprise_Security_Strategic_Plan_101509085921_Enterprise_Strategic_Plan_091008101051_EnterpriseSecurityStrategicPlan_FY2009-2013.pdf**) and
  - Minnesota Enterprise Security Tactical Plan (**http://www.state.mn.us/mn/externalDocs/OETnet/Enterprise_Security_Tactical_Plan_101509095517_ESO_TacticalPlan.pdf**)

- Are the departments mandated to use the provided services?

  For those services determined to be enterprise-wide utility services, agencies will be required to use those services.

- How many data centers are currently in use by the state?

  The state has 37 defined data centers.

- Is each organization including the Executive Branch responsible for its own information security risk management program?

  Yes, this is the current practice.

- According to NIST-SP800-35 section 3, paragraph 3.1, will OET provide Management, Operational and Technical services?

  Yes.

- Does a catalog of specific services exists that describes what OET can provide to an organization? Can this catalog of services be shared to assist in answering the SOW questions?

  OET offers many centralized solutions to the serve the business needs of government entities. A catalog of services offered can be found at: **http://www.state.mn.us/portal/mn/jsp/content.do?id=-536890274&agency=OETweb**

- Will OET be responsible for the on-going third-party management of any external services provided to an organization?

  Security oversight of third-party providers is a relatively immature process and fragmented across the Executive Branch. This study should assist with providing an answer as to what role OET will provide in the future.

- What third-party management process does OET currently follow? (e.g. BITS FISAP, ISO 27001, VRR)

  No standard methodology has been defined.

- Is OET currently designed to be a Managed Security Service Provider (MSSP) for other organizations?

  Some security services are being provided to government entities outside of the Executive Branch.

- What (whose) policies and standards will be followed if an organization chooses to utilize one or more services?

Enterprise policies and standards will define a minimum threshold to be followed. Government entities may choose to have more stringent standards.

- Are there any existing design-plans that exists that will help facilitate "Operational Practices"? (e.g. Incident Management, RACI, Breech Notification)

  OET operational practices are based upon the Information Technology Information Library (ITIL) process framework. Various projects have been initiated over the past year to assist with designing these practices.

- What process does OET follow for conducting an Information Security Risk Assessment? (e.g. identify critical assets, security requirements, threat analysis, risk metrics, etc.)

  Enterprise information risk assessment processes are in a development phase; however, all security processes are being based upon the NIST framework.

- Besides NIST as a standard for security government computing systems, what other standards are being followed? What governance model is generally being followed? And what is favored by OET? Has the state selected a preferred security framework?

  The Enterprise Security program considers many industry best practice frameworks, but it is based upon the NIST security framework. The IT governance model can be found at: **http://www.state.mn.us/portal/mn/jsp/content.do?subchannel=-536895827&programid=536918780&sc3=null&sc2=null&id=-536895826&agency=OETweb**

- Has OET previously taken full, partial or specific risk management over for an organization?

  The Enterprise Security program staff provide full security risk management services only for the operational components performed by the Office of Enterprise Technology.

- Has any type of Business Case (communication), Cost-Benefit Analysis (Evaluation) and Return on Investment (Valuation) even been completed for any organization wishing to utilized OET existing services?

Yes.

- Does a Business Impact Analysis exist and what organizations does it cover? Can any portion of the BIA be shared to assist in answering the SOW?

  Business Impact Analysis' exist for approximately 50 Executive Branch agencies, boards, and commissions. Due to the sensitive nature of these documents, they cannot be shared as part of the SOW process.

- Is there a document that describes OET's accounting practices?

  The State of Minnesota follows generally accepted accounting principles, as defined by the Governmental Accounting Standards Board (GASB). A document that helps articulate the accounting position of the state is the Comprehensive Annual Financial Report, published by the Minnesota Management & Budget. Those reports can be found at **http://www.mmb.state.mn.us/fin/acct** . The Office of Enterprise Technology reports most of its financial activities in the Enterprise Technology Revolving Fund.

- Over what span of time will the meetings to discuss and present the results with government leaders and legislators occur?

  Meetings to discuss and present the results could happen throughout the 2010 Legislative Session (February – May).

- Please confirm that all on-site visits are local to St. Paul/Minneapolis.

  The majority of the work is expected to be performed at the Office of Enterprise Technology, located at 658 Cedar Street, St. Paul, Minnesota. However because this is an enterprise funding study, the respondent should consider interactions with government entities located outside of the St. Paul/Minneapolis metro area.

- The SOW states that projected scope, methodology and work breakdown structure is part of the deliverable and must be reviewed and approved by OET no later than November 30, 2009. It also states that the completed strategy document must be delivered to OET by February 5, 2010. Finally, it states that responses to the SOW are due November 10, 2009. Is there some flexibility in these dates?

Consideration of staffing, availability and deliverables will be considered during the evaluation process. Meeting the deliverable deadlines will be crucial as OET is legislatively mandated to present a report by March 15, 2010. All responses are due by 2:00 PM CDT on November 10, 2009.

- It is hard to tell if this is really a project-based or staffing-based SOW. For the cost proposal, please confirm that you are only looking for a proposed hourly rate, and that you do not expect an overall estimate for the work effort.

  OET is looking of a hybrid cost proposal; one that includes hourly rates and résumés for proposed staff, with an estimate number of staff and hours the respondent feels necessary to deliver a completed strategy document by February 5, 2010.

- Must an organization be registered in all three of the Master Contract Vendor Service Categories listed on the title page of this statement of work before it can respond?

  No. The respondent need only be registered in any one of the three eligible service categories.

- What technologies does this project cover?

  The State of Minnesota utilizes a vast array of technologies to deliver its services. This project should consider all existing and potential future technologies.

- What specific technical skills and compliance expertise would the selected candidate require to have?

  Respondents must possess the minimum Required Skills and should possess the Desired Skills as defined on page 4 and 5 of the SOW. Candidates should have knowledge of various compliance requirements, including but not limited to FISMA, HIPAA, PCI DSS, CIPA, FERPA, and IRS Federal Tax mandates.